Jurnal Inkofar * Volume 1 No. 1, Juli 2020 * ISSN: 2615-3645 (Print) / 2581-2920 (Online)
Tersedia secara online di: http://www.politeknikmeta.ac.id/meta/ojs/

IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA PADA LINUX DEBIAN 9 BERBASIS CLOUD VIRTUAL PRIVATE SERVERS (VPS)

Mamay Syani
Jurusan Teknik Komputer dan Informatika/ Politeknik TEDC Bandung /
msyani@poltektedc.ac.id

ABSTRACT
The development of information technology, especially on virtual Private server (VPS) technology in particular that uses Debian Linux operating system, increasingly facilitated with the service Adaya of some VPS providers both locally and non-local, but there is a problem vulnerability if, the server maintainers do not shame testing against the resilience of attacks from outside parties, with the Network Development Life Cycle (NDLC) method is one of the most popular in the Monitoring phase is using Suricata Intrusion Detection System (IDS) software. Suricata is a tool to detect any suspicious activity that could be threatening a network or server with Brute Force technique, DDOS, Port Scanning. Suricata is able to display logs from suspicious activity results in detail with the time, date and IP address of the activity even with the tools used to perform the activity. Also suricata can detect if there is suspicious activity associated with the network.
Keywords : *IDS, Suricata, Debian, Brute Force, DDOS, Port Scanning.*

ABSTRAK
Perkembangan Teknologi Informasi, khsusnya pada teknologi virtual private server (VPS) khususnya yang menggunakan system operasi linux Debian, semakin dimudahkan dengan adaya layanan dari beberapa penyedia VPS baik lokal mapun non lokal, tetapi terdapat masalah kerentanan apabila, para pengelola server tidak Malukan pengujian terlebih dahulu terhadap ketahanan serangan dari pihak luar, dengan metode Network Development life Cycle (NDLC) salah yang paling popular dalam tahapan Monitoring yaitu menggunakan software Intrusion Detection System (IDS) Suricata. Suricata merupakan tools untuk mendeteksi adanya aktivitas - aktivitas yang mencurigakan yang bisa jadi mengancam jaringan atau server dengan Teknik *Brute Force, DDOS, Port Scanning* . Suricata mampu menampilkan log - log dari hasil aktivitas yang mencurigakan secara detail dengan waktu, tanggal dan alamat IP yang melakukan aktivitas tersebut bahkan dengan tools yang digunakan untuk melakukan aktivitas tersebut. Selain itu juga suricata bisa mendeteksi jika ada aktivitas mencurigakan yang berhubungan dengan jaringan.
Kata Kunci : *IDS, Suricata, Debian, Brute Force, DDOS, Port Scanning.*

1. PENDAHULUAN
Perkembangan Teknologi Informasi, khususnya pada teknologi virtual private server (VPS) khususnya yang menggunakan system operasi linux Debian, semakin dimudahkan dengan adaya layanan dari beberapa penyedia VPS baik lokal mapun non lokal, tetapi terdapat masalah kerentanan apabila, para pengelola server tidak Malukan pengujian terlebih dahulu terhadap ketahanan serangan dari pihak luar, dengan metode Network Development life Cycle (NDLC) Hal ini membuat seseorang secara ilegal untuk masuk ke dalam sistem dan membuat lumpuh sistem tersebut. Selain itu, adanya celah dan tidak adanya sistem keamanan yang melindungi sistem menjadikan sistem rentan terhadap serangan. Keamanan menjadi suatu hal penting yang melindungi suatu informasi atau data, demi keamanan data masyarakat akan teknologi dan ancaman informasi pada Cloud Computing sangat beragam mulai dari scanning Port, Backdoor, Brute Force hingga

penyerangan Denial Of Service (DOS). Ancaman informasi tersebut menyebabkan server akan mati dan tidak dapat beroperasi lagi sehingga otomatis tidak dapat memberikan pelayanan. Serangan-serangan tersebut dapat bertujuan untuk mengakses sistem aplikasi atau mencoba masuk ke dalam jaringan dengan hak akses khusus hingga mengakses sumber daya atau layanan yang disediakan baik dalam sistem atau jaringan. Suricata merupakan Intrusion Detection System (IDS) yang dapat mendeteksi aktifitas ancaman serangan pada jaringan yang dibantu dengan rules yang telah ada. Cara kerja dari suricata adalah ketika adanya penyerangan suricata akan melakukan pengecekan paket/serangan yang ada melalui rules yang dibuat. Ketika serangan terdeteksi maka suricata akan membuat log serangan yang dilakukan, Suricata juga dapat melakukan deteksi otomatis pada layer 7 yaitu aplikasi seperti dns, http, imap, ftp, dan smtp. Sehingga Suricata dapat memberikan solusi untuk meningkatkan keamanan dalam Cloud Computing berbasis linux Debian. Berdasarkan uraian diatas maka penulis implementasi intrusion detection system (IDS) menggunakan suricata pada linux Debian 9 berbasis cloud Virtual Private Servers (VPS)

2. KAJIAN PUSTAKA

A. Intrusion Detection System (IDS)

IDS merupakan program atau aplikasi yang dapat mendeteksi adanya gangguan pada sistem. Pada saat ini ada beberapa IDS yang umum digunakan pada jaringan, salah satunya adalah suricata. Adapun tujuan dari tools ini diantaranya: mengawasi jika terjadi penetrasi ke dalam sistem, mengawasi traffic yang terjadi pada jaringan, mendeteksi anomali terjadinya penyimpangan dari sistem yang normal atau tingkah laku user, mendeteksi signature dan membedakan pola antara signature user dengan attacker. IDS juga memiliki cara kerja dalam menganalisa apakah paket data yang dianggap sebagai intrusion oleh intruder. Cara kerja IDS dibagi menjadi dua, yaitu, Knowledge Based dan Behavior Based. (Mell, P., & Grance, T. (2012).).

B. Virtual Private Sever

Virtual Private Server (VPS) adalah teknologi virtualisasi dimana anda bisa memiliki sebuah *server virtual* yang *resource Central processing unit* (CPU) , *Random-access memory* (RAM), dan *Storage*nya dialokasikan secara pasti tanpa harus memiliki server secara fisik. Teknologi ini memungkinkan Anda untuk memiliki akses *root* dan meng *custom server* sesuai dengan kebutuhan anda. Tentu dengan biaya yang jauh lebih murah dibandingkan jika anda menyewa *dedicated server*. Dalam layanan VPS ini, satu server induk dengan spesifikasi yang tinggi (*Dual Processor – Multiple Core*) dibagi-bagi resourcenya menjadi beberapa *server virtual* (*Virtual Private Server* / VPS) dimana antar *server virtual* bekerja secara bersamaan, bahkan dengan *Operating system* (OS) yang berbeda-beda tanpa adanya kemungkinan untuk saling mengganggu satu sama lain. (Medeni, I. (2016).

C. Suricata

Suricata merupakan network based intrusion detection and prevention system yaitu suatu perangkat lunak yang dapat digunakan untuk mendeteksi dan mencegah (Detection System dan Prevention System) terhadap lalu lintas sebuah jaringan. Suricata adalah IDS open source yang dikembangkan oleh Open Information Security Foundation (OISF) (Bhosale, D.A & Mane, V.M 2015).

D. Brute Force

Brute Force adalah jenis serangan yang bertujuan untuk mencoba segala kemungkinan kombinasi karakter untuk mencari account yang valid. Brute force attack masih menjadi salah satu teknik cracking password paling populer yang dilakukan untuk meretas kata sandi. Serangan ini dilakukan agar peretas memiliki akses tidak sah untuk bisa masuk ke dalam sistem. (Grover, V. (2020)

E. DDoS Attack

DDos Attack merupakan sebuah metode serangan dengan mengirimkan banyak paket ke dalam dalam sebuah jaringan yang menyebabkan perangkat jaringan tidak lagi dapat berjalan sesuai fungsinya dan dibutuhkan sebuah metode untuk mendeteksi kejadian pada server secara real-time agar dapat dianalisa dan menjadi dasar sebagai alat bukti yaitu dengan menggunakan Intrusion Detection System (IDS) pada server (Ridho, Yudhana dan Riadi, 2016). DDoS disebut sebagai senjata pilihan hacker karena telah terbukti menjadi ancaman permanen bagi pengguna, organisasi dan infrastruktur di Internet (Business Week, 2014). Di sisi lain, serangan jaringan merupakan risiko

untuk integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi (Zhao et.al, 2015).

F. Port Scanning

Port Scanning merupakan ancaman yang cukup serius bagi suatu sistem jaringan komputer, dan menjadi hal yang sangat menguntungkan bagi para attacker. Dengan Port Scanning, attacker mendapatkan informasi-informasi berharga yang dibutuhkan dalam melakukan serangan. Dengan kata lain, melakukan Port Scanning ialah untuk mengidentifikasi port-port yang terbuka, dan mengenali OS (Operating System) target. Asaduzzaman, M., Rawshan, P. P., Liya, N. N., Islam, M. N., & Dutta, N. K. (2020, February).

G. Sistem Operasi Debian

Debian adalah sistem operasi free (dari kata freedom yang berarti kebebasan) untuk komputer anda. Sistem operasi adalah sekumpulan program-program dasar dan berbagai utilitas yang diperlukan komputer anda untuk bisa bekerja. Debian tidak hanya sekedar menyediakan sistem operasi: tetapi juga lebih dari 59000 paket-paket lainnya, berupa berbagai perangkat lunak terkompilasi yang dikemas dengan baik untuk memudahkan instalasi. (Claes, M., Mens, T., Di Cosmo, R., & Vouillon, J. (2015, May)

H. Network Development Life Cycle

Network Development Life Cycle (NDLC) merupakan suatu metode yang digunakan dalam mengembangkan atau merancang jaringan infrastruktur yang memungkinkan terjadinya pemantauan jaringan untuk mengetahui statistik dan kinerja jaringan, metode ini bersifat continous improvment dimana hasil dari analisis akan terus dijadikan sebagai bahan pertimbangan untuk melakukan perbaikan terus menerus. (Prabowo, R. T., & Kurniawan, M. T. (2015)

3. HASIL DAN PEMBAHASAN

A. Metode Penelitian

Pada bab ini berisikan tahapan dalam menyelesaikan penelitian yang berjudul Implementasi Intrusion Detection System (IDS) menggunakan suricata pada linux debian 9 berbasis cloud Virtual Private Servers (VPS). Bab ini berfungsi sebagai panduan alur pengerjaan dalam penelitian yang ditunjukan agar penelitian berjalan dengan sesuai harapan. Tahapan tersebut berupa langkah-langkah yang akan dilakukan dalam penelitian secara sistematis dan spesifik. Berikut merupakan gambaran metodologi berupa flowchart yang ditunjukan pada Gambar 1

Gambar 3.1 Flowchart Metodologi Penelitian

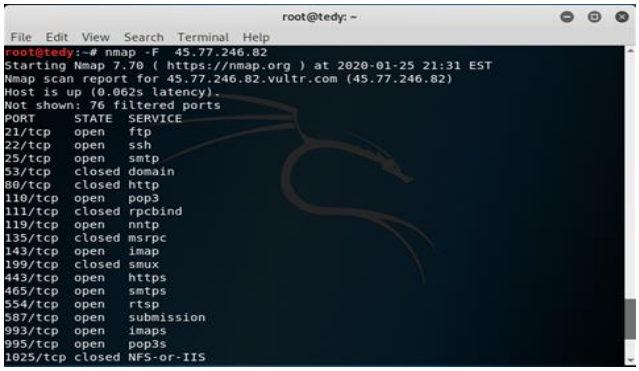
Adapaun penjelasan dari flowchart tersebut sebagai berikut:

1) *Studi literatur:* digunakan sebagai pedoman pengetahuan dasar dalam melakukan analisis, perancangan, implementasi dan pengujian dalam tahap-tahap penelitian. Dasar teori yang dibutuhkan sebagai pendukung penelitian ini adalah *Open Source*, IDS, IDS Suricata, VPS, dan *tools* Suricata
2) *Membangun lingkungan pengujian:* segala komponen-komponen dan ketubtuhan perangkat lunak uji coba dirancang pada tahap ini.
3) *Melakukan pengujian dan pengambilan hasil data uji:* pengujian yang dilakukan adalah dengan melakukan pengujian selama dua hari dalam kurun waktu satu mingu, kemudian melihat log yang dihasilkan dari penyerangan yang sudah dilakukan dan sudah berhasil menyerang target.
4) *Penutup:* berisi kesimpulan dari penelitian yang dilakukan sesuai dengan ruang lingkup pengujian. Bagian ini juga berisi saran untuk penelitian kedepannya.

B. Jenis-jenis Serangan Terhadap Sistem Keamanan

Berbagai cara dilakukan oleh PC attacker untuk menguji kehandalan dari sistem keamanan open cloud berbasiskan IDS dan IPS ini. Jenis-jenis serangan yang dilakukan, antara lain yaitu *brute force*, *scanning*, dan D-DoS (*Denial of Service*). Dengan memanfaatkan beberapa tools pengujian, sistem keamanan ini akan diuji dengan menggunakan beberapa tools untuk melakukan hacking ke beberapa komputer target yang ditentukan. Dalam hal ini komputer yang menjadi target yaitu komputer server menggunakan sistem operasi Debian 9 server dengan IP address 45.77.246.82 yang menjalankan layanan web server.

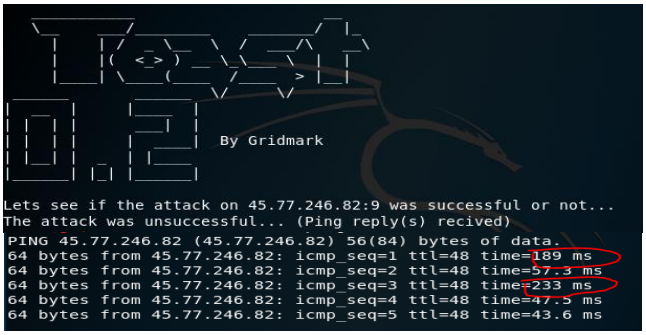
1. Port Scanning



Gambar 3.2 Port Scanning menggunakan nmap

Pengujian serangan pertama terhadap sistem keamanan open cloud berbasiskan IDS menggunakan cloud computing. Dalam hal ini attacker melakukan proses nmap terhadap komputer yang terdapat di jaringan server untuk mengetahui port-port yang terbuka dan OS yang digunakan server yang menjadi target serangan.

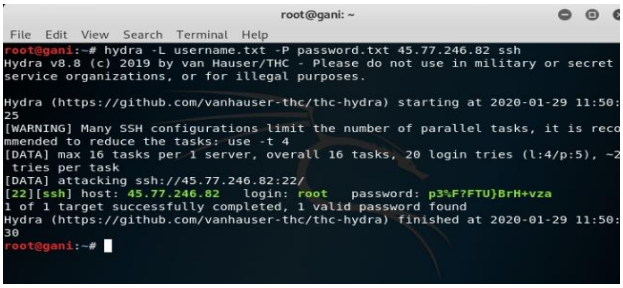
2. DDos Attack



Gambar 3.3 DDos Attack menggunakan TOAST

Pengujian serangan metode DDos dengan menggunakan tools Toast dilakukan untuk menguji apakah suricata dapat menangkap aktivitas ini atau tidak dikarenakan aktivitas ini merupakan aktivitas yang berbahaya untuk jaringan atau server.

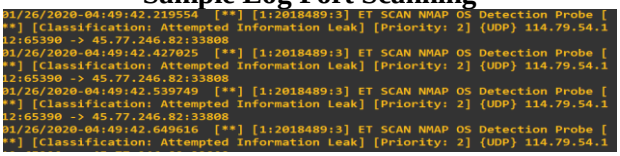
3. Brute Force



Gambar 3.4 Brute Force menggunakan Hydra

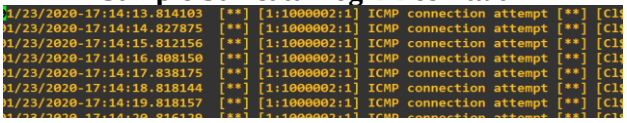
Pengujian serangan metode *brute force* dengan menggunakan tools Hydra dilakukan untuk menguji keamanan terhadap data username dan password.

Sample Log Port Scanning



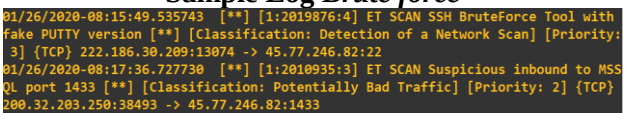
Gambar 3.5 Sistem mendeteksi penyerangan network scanning

Sample Suricata Log DDos *Attack*



Gambar 3.6 Sistem mendeteksi penyerangan DDOS

Sample Log *Brute force*



Gambar 3.7 Sistem mendeteksi penyerangan *Brute force*

C. Pembahasan

Pembahasan yang akan disajikan ini meliputi hasil log serangan Port *Scanning*, DDoS dan *Brute Force*. Hasil yang ditampilkan adalah hasil selama satu minggu (dari tanggal 20 - 26 Januari 2020) penyerangan yang dilakukan ke VPS dengan alamat IP 45.77.246.82.

1. Brute Force

Berikut adalah hasil log suricata dari serangan yang dilancarkan ke Server selama satu minggu menggunakan metode Brute Force.

Tabel 3.1. Log Suricata dari hasil Brute Force Attack

No	Jenis Penyerangan	Tanggal	Jumlah
1	Brute Force	20-01-2020	2
2	Brute Force	21-01-2020	1
3	Brute Force	22-01-2020	5
4	Brute Force	23-01-2020	4
5	Brute Force	24-01-2020	2
6	Brute Force	25-01-2020	2
7	Brute Force	26-01-2020	3
Total			**19**

2. DDos Attack

Berikut adalah hasil log suricata dari serangan yang dilancarkan ke Server selama satu minggu menggunakan metode DDos.

Tabel 3.2. Log Suricata dari hasil DDos Attack

No	Jenis Penyerangan	Tanggal	Jumlah
1	DDos Attack	20-01-2020	4
2	DDos Attack	21-01-2020	3
3	DDos Attack	22-01-2020	4
4	DDos Attack	23-01-2020	3
5	DDos Attack	24-01-2020	5
6	DDos Attack	25-01-2020	6
7	DDos Attack	26-01-2020	6
Total			**31**

3. Port Scanning

Berikut adalah hasil log suricata dari serangan yang dilancarkan ke Server selama satu minggu menggunakan metode Port Scanning.

Tabel 3.3. Log Suricata dari hasil Port Scanning

No	Jenis Penyerangan	Tanggal	Jumlah
1	Port Scanning	20-01-2020	5
2	Port Scanning	21-01-2020	5
3	Port Scanning	22-01-2020	6
4	Port Scanning	23-01-2020	4
5	Port Scanning	24-01-2020	6
6	Port Scanning	25-01-2020	6
7	Port Scanning	26-01-2020	6
Total			**36**

D. Evaluasi Hasil

Dari hasil yang telah dipaparkan di tabel 3.1, 3.2, dan 3.3, Suricata sangat berperan penting untuk keamanan cloud virtual private server dari serangan - serangan yang tidak bertanggung jawab. Dengan adanya suricata, seorang yang bertanggung jawab terhadap server dapat mengatasi atau mengantisipasi serangan- serangan yang datang. Dapat dilihat pada table, bahwa dalam satu minggu saja banyaknya serangan yang dilancarkan kepada server berjumlah 86. Port Scanning mendominasi banyaknya jumlah serangan dari ketika metode penyerangan (Brute Force, DDos dan Port Scanning), dikarenakan untuk melakukan Brute force diperlukan port scanning terlebih dahulu. DDos Attack juga banyak dilancarkan dikarenakan DDos merupakan serangan yang dapat membuat server menjadi *down* dikarenakan dalam satu kali serangan DDos saja dapat dilipat gandakan *request* nya sehingga menjadi overload dan akhirnya server down bahkan bisa jadi tidak bisa di akses. Oleh karena itu suricata adalah salah satu solusi untuk menangani serangan - serangan yang tidak bertanggung jawab kepada server.

4. KESIMPULAN

Kesimpulan yang dapat diperoleh dari penelitian terkait implementasi IDS menggunakan suricata adalah sebagai berikut:

Server IDS mampu menerapkan Suricata dengan motode inline afpacket yang dapat mengindentifikasi jenis-jenis serangan yang terjadi di dalam jaringan. yaitu brute force, scanning dan D-DoS yang dapat menampilkan alerts yang tercatat pada log pada suricata.

5. DAFTAR PUSTAKA

Mell, P., & Grance, T. (2012). The NIST definition of cloud computing: Recommendations of the national institute of standards and technology (2011). NIST Special Publication, 800-145.

Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing: Recommendations of the national institute of standards and technology (2011)." NIST Special Publication (2012): 800-145.
Medeni, I. (2016). VIRTUAL PRIVATE SERVER OR MICRO PCS: WHICH IS BETTER FOR THE LEARNING MANAGEMENT SYSTEM DECISION?.
Bhosale, D.A. & Mane, V.M, "Comparative Study and Analysis of Network Intrusion Detection Tools,"
Cho, J. S., Yeo, S. S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer communications, 34(3), 391-397.
Zhao, T., Lo, D. C.-T., & Qian, K. (2015). A Neural Network Based DDoS Detection System Using Hadoop and HBase. IEEE 17th International Conference on High Performance Computing and Communication, 1326-1331.
Fouladi, R. F., Kayatas, C. E., & Anarim, E. (2016, June). Frequency based DDoS attack detection approach using naive Bayes classification. In 2016 39th International Conference on Telecommunications and Signal Processing (TSP) (pp. 104-107). IEEE.
Grover, V. (2020). An Efficient Brute Force Attack Handling Techniques for Server Virtualization. Available at SSRN 3564447.
Asaduzzaman, M., Rawshan, P. P., Liya, N. N., Islam, M. N., & Dutta, N. K. (2020, February). A vulnerability detection framework for cms using port scanning technique. In International Conference on Cyber Security and Computer Science (pp. 128-139). Springer, Cham.
Claes, M., Mens, T., Di Cosmo, R., & Vouillon, J. (2015, May). A historical analysis of debian package incompatibilities. In 2015 IEEE/ACM 12th Working Conference on Mining Software Repositories (pp. 212-223). IEEE.

